

WHAT IS CLAIMED IS:

1 1. A DNS server filter apparatus comprising:
2 packet verification means for verifying whether
3 there is any abnormality in contents of a received DNS
4 (domain name system) packet before transmitting it to a
5 DNS server; and
6 error response means for generating an error
7 response packet and transmitting it to a request source if
8 an abnormality is detected.

1 2. A DNS server filter apparatus claimed in Claim
2 1:
3 wherein said packet verification means checks a DNS
4 packet for obtaining information on a host name, a domain
5 name, and an IP (Internet protocol) address transmitted
6 from a network outside an organization by a person outside
7 the organization using a DNS protocol; and
8 wherein said error response means generates an error
9 response packet and transmits it to a request source when
10 detecting an abnormality, thereby preventing the person
11 outside the organization from invading a network of the
12 organization by using private information of the
13 organization and preventing the DNS server from operating
14 abnormally by receiving a packet having an abnormal format.

1 3. A DNS server filter apparatus claimed in Claim
2 1:

09750914.010201

wherein said packet verification means checks a DNS packet for obtaining information on a host name, a domain name, and an IP address transmitted to a DNS server belonging to a network outside the organization from a terminal inside the organization using the DNS protocol; and

wherein said error response means generates an error response packet and transmits it to a request source when detecting an abnormality, thereby preventing said DNS server belonging to the network outside the organization from operating abnormally.

4. A DNS server filter apparatus claimed in one of Claims 1 to 3, further comprising:

adding and deleting means for adding or deleting abnormality detecting conditions of the DNS packet.

5. A firewall apparatus wherein there is mounted said DNS server filter apparatus claimed in one of Claims 1 to 4.

6. A network system, further comprising:
a packet filtering firewall apparatus;
a DNS packet filter apparatus according to one of Claims 1 to 4 to communicate with the firewall apparatus;
and
a DNS server for communicating with said DNS packet

09750914.010201

7 filter apparatus.

1 7. A DNS server filter apparatus comprising:
2 a packet receiving section for receiving an inquiry
3 from a terminal or a DNS server and a response packet from
4 a DNS server;
5 a session management section for managing inquiry
6 packets and response packets for an entire control, having
7 a session management table for managing inquiry requests;
8 a packet verification section for verifying whether
9 the inquiry packet or the response packet is abnormal;
10 a request generating section for generating an
11 inquiry packet to the DNS server;
12 a response generating section for generating a
13 response packet to be returned to a transmission source of
14 the inquiry packet;
15 a packet transmitting section for transmitting the
16 inquiry packet and the response packet; and
17 response means for verifying whether there is any
18 abnormality in contents of the received packet in a DNS
19 protocol before transmitting the packet to the DNS server
20 regarding the received packet in the DNS protocol and
21 generating an error response packet to transmit it to a
22 request source if an abnormality is detected.

1 8. A DNS server filter apparatus claimed in Claim
2 7:

09750914-010201

3 wherein said packet verification section comprises;
4 a calling management section for controlling
5 operations of selecting and executing a verification
6 program to be executed by referring to an attribute of
7 said verification program, having a program management
8 table containing entry point address information of the
9 verification program, priority information of executing
10 the verification program, and attribute information of the
11 verification program;

12 a storage device in which the verification program
13 is stored;

14 a load management section for loading an execution
15 file of a verification program specified by a management
16 tool or by a setting file on a memory, for initializing
17 the loaded verification program, for registering an entry
18 point of the verification program onto said program
19 management table of said calling management section
20 together with the obtained attribute, and for controlling
21 a verification program specified to be deleted by said
22 management tool so as to be released; and

23 a service routine comprising a subroutine group for
24 utilizing functions of a DNS server filter body called by
25 the executed verification program.

1 9. A DNS server filer apparatus claimed in Claim 8:

2 wherein said session management table comprises a
3 pointer to a request packet, an IP address of a request

09750944-010201

4 source which has issued an inquiry request, a port number
5 of the request source which has issued the inquiry request,
6 and a flag indicating whether the inquiry request has been
7 transferred to another DNS server if the inquiry request
8 has a normal packet format;

9 wherein said packet receiving section receives a DNS
10 packet and then transmits the packet to said session
11 management section; and

12 wherein said session management section makes
13 settings of an IP address of a transmission source of the
14 received packet, a port number of the received packet, and
15 a flag value indicating "Testing" in said session
16 management table, transmits the received packet to said
17 packet verification section to request a packet
18 verification, checks a type of said received packet to
19 judge whether it is an inquiry request if there is any
20 problem in contents of the verification as a result of the
21 verification of said received packet in said packet
22 verification section;

23 wherein if it is judged to be an inquiry request as
24 a result of the judgement, the session management section
25 requests said response generating section to generate an
26 error response packet, requests said packet transmitting
27 section to transmit the generated packet to a destination
28 specified by the request source IP address and the request
29 source port number on said session management table, and
30 deletes information registered in said session management

09750914-010201

31 table regarding the received packet to release the
32 received inquiry request packet; and
33 wherein unless it is an inquiry request, the session
34 management section searches said session management table
35 to fetch a part related to an original inquiry request,
36 requests said response generating section to generate an
37 error response packet based upon an inquiry request packet
38 by referring to the inquiry packet from the request packet
39 pointer of an entry of said searched session management
40 table, requests said packet transmitting section to
41 transmit the generated response packet to a destination
42 specified by the request source IP address and the request
43 source port number on said session management table,
44 deletes information registered in said session management
45 table regarding the received response packet to release
46 the response packet and deletes the entry registered in
47 said session management table regarding the inquiry
48 request corresponding to the response packet.

1 10. A DNS server filter apparatus claimed in Claim
2 9:

3 wherein said session management section checks a
4 type of the received packet if there is no problem as a
5 result of the packet verification performed in said packet
6 verification section, searches said session management
7 table for information on the inquiry request corresponding
8 to the response packet if it is a response packet, and

09750944-010204

9 verifies whether the received response packet can be a
10 response to the original inquiry request;

11 wherein if there is a need for making an additional
12 inquiry as a result of said verification, said session
13 management section determines the next inquiry destination
14 from the information of the received response packet,
15 requests said request generating section to generate an
16 inquiry request packet, requests said packet transmitting
17 section to transmit it to the next inquiry destination,
18 and deletes information on the response packet in progress
19 of the received inquiry from said session management table
20 to release the response packet; and

21 wherein if the received response packet can be a
22 response to the original inquiry request packet as a
23 result of said verification, the session management
24 section requests said response generating section to
25 generate a response packet to the original inquiry request
26 reflecting the result of the response packet of receiving
27 the response packet, requests said packet transmitting
28 section to transmit it to the transmission source of the
29 original inquiry request, deletes information related to
30 the received response packet from said session management
31 table, and deletes information related to the original
32 inquiry request from said session management table to
33 release the response packet.

1 11. A DNS server filter apparatus claimed in Claim

2 9 or 10:

3 wherein said session management section checks a
4 type of the received packet if there is no problem as a
5 result of the packet verification in said packet
6 verification section, checks a transmission source of the
7 received packet if the received packet is an inquiry
8 request and then unless said transmission source is a
9 network inside an organization issuing an inquiry,
10 determines a DNS server outside the organization to which
11 an inquiry is issued first to meet the inquiry request of
12 a network outside the organization, requests said request
13 generating section to generate an inquiry request based
14 upon the original inquiry request, and requests said
15 packet transmitting section to transmit the inquiry to
16 said determined DNS server, or if said transmission source
17 is the network inside the organization issuing the inquiry,
18 requests said request generating section to generate an
19 inquiry request packet base upon the received inquiry
20 request packet, requests said packet transmitting section
21 to transmit the inquiry packet to the DNS server, sets a
22 "Inquiring" value to the flag among the entries of said
23 session management table corresponding to the received
24 packet, and sets a pointer to the received packet to the
25 pointer of the entry on said session management table.

1 12. A DNS server filter apparatus claimed in Claim
2 7, wherein a cache memory previously stores DNS server

09750914-010201
102070-4605260

3 information.

1 13. A record medium having a program recorded
2 therein and capable of executing:

3 packet receiving processing for receiving an inquiry
4 from a terminal or a DNS server in the DNS protocol and a
5 response packet from a DNS server via a communication
6 apparatus;

7 session management processing for managing inquiries
8 and response packets for an entire control, having a
9 session management table for managing the inquiry
10 requests;

11 packet verification processing for verifying whether
12 an inquiry or a response packet is abnormal;

13 request generation processing for generating an
14 inquiry packet to a DNS server;

15 response generation processing for generating an
16 inquiry packet to the DNS server;

17 response generation processing for generating a
18 response packet to be returned to a transmission source of
19 the inquiry packet;

20 packet transmission processing for controlling an
21 operation so as to transmit an inquiry and a response
22 packet through a communication apparatus; and

23 DNS server filter processing for verifying whether
24 there is any abnormality in contents of the packet before
25 transmitting the packet to the DNS server regarding the

09750914.010201

26 received DNS packet; if an abnormality is detected, it
27 generates and transmits an error response packet.

1 14. A record medium claimed in Claim 13, having a
2 program recorded therein and capable of executing:

3 wherein said program management table comprises
4 entry point address information of the verification
5 program, priority information of executing the
6 verification program, and attribute information of the
7 verification program;

8 wherein the calling management processing is
9 performed for selecting and executing a verification
10 program to be executed by referring to the attribute of
11 said verification software; and

12 wherein the load management processing is performed
13 for loading an execution file of the verification program
14 specified by a management tool or a setting file on a
15 memory, for initializing the loaded verification program,
16 for registering an entry point of the verification program
17 together with an obtained attribute on said program
18 management table, and for releasing a verification program
19 specified to be deleted by said management tool from the
20 memory.

1 15. A group of recording media, wherein said
2 program claimed in Claim 13 is divided into a plurality of
3 portions and said portions are recorded on said media,

09750914-010001
12010-1165260

4 respectively.

1 16. A group of recording media, wherein said
2 program claimed in Claim 14 is divided into a plurality of
3 portions and said portions are recorded on said media,
4 respectively.

1 17. A program embodied as electric signals,
2 comprising:
3 packet receiving processing for receiving an inquiry
4 from a terminal or a DNS server in the DNS protocol and a
5 response packet from the DNS server via a communication
6 apparatus;

7 session management processing for managing the
8 inquiry and the response packet for an entire control
9 using a session management table for managing inquiry
10 requests;

11 packet verification processing for verifying whether
12 the inquiry and the response packet are abnormal;
13 request generation processing for generating an
14 inquiry packet to the DNS server;

15 response generation processing for generating a
16 response packet returned to a transmission source of the
17 inquiry packet;

18 packet transmission processing for controlling an
19 operation to transmit the inquiry and the response packet
20 via the communication apparatus; and

09750914.010201

21 DNS server filter processing for verifying whether
22 there is any abnormality in contents of the received DNS
23 packet before transmitting the packet to the DNS server
24 regarding the received DNS packet and for generating and
25 transmitting an error response packet when detecting an
26 abnormality.

1 18. A program claimed in Claim 17 embodied as
2 electric signals, further comprising:

3 a program management table having entry point
4 address information of the verification program, priority
5 information for executing the verification program, and
6 attribute information of the verification program,
7 calling management processing for selecting and
8 executing a verification program to be executed by
9 referring to the attribute of said verification software;
10 and

11 load management processing for loading an execution
12 file of the verification program specified by a management
13 tool or a setting file on a memory, for initializing the
14 loaded verification program, for registering an entry
15 point of the verification program together with the
16 obtained attribute on said program management table, and
17 for releasing the verification program specified to be
18 deleted by said management tool from the memory.

09750914.010201